UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,157	11/03/2003	Robert N. Nazzal	12221-026001	5548

26161 7590 10/14/2008

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
GEE, JASON KAI YIN	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
10/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/701,157
Filing Date: November 03, 2003
Appellant(s): NAZZAL, ROBERT N.

Denis G. Maloney (29,670)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 08/08/08 appealing from the Office action mailed 02/08/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct

.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0069200	COOPER	6-2002
6,986,161	BILLHARTZ	1-2006
6,321,338	PORRAS	11-2001
5,550,807	KUROSHITA	8-1996

Symantec. "Symantec Antivirus for Macintosh." 1992. Pages 4-9, 4-10, 5-6, and 5-7.

Central Point. "Central Point Anti-Virus – Virus detection, removal, and Prevention."

1991. Pages. 46-47

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-9 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper US Patent Application Publication 2002/0069200 (hereinafter Cooper), and

in view of Symantec's *Symantec Antivirus for Macintosh SAM*, 1994, (hereinafter Symantec).

As per claim 1, Cooper teaches a graphical user interface rendered on a display associated with an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event that is detected in a network (throughout the reference, such as Figure 26, paragraph 514, abstract, paragraph 42), the summary indicating event severity details of the event (Figure 26). However, at the time of the invention, Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time. A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.

At the time of the invention, it would have been obvious to combine the teachings of Cooper with Symantec. One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.

As per claim 2, Symantec teaches wherein the snooze control feature can be selected based on event types (4-9 and 5-6, such as when events occur when copying

programs). Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.

As per claim 3, Symantec teaches clearing alerts if the alerts appear on the overview page (pages 5-6 and 4-9). Also, this is taught by Cooper in Figure 28, wherealerts may be cleared on an overview page with an aggregated view of the network status.

As per claim 4, Cooper teaches wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event (Figure 22).

As per claim 5, Cooper teaches wherein details of events include values of source (Figure 23), destination (Figure 23), and protocol that caused an event to be raised (Figure 24).

As per claim 6, Cooper teaches wherein event severity is coded by an indicia (Figures 22, 25, 26, paragraph 520).

As per claim 7, Symantec teaches a control to clear a selected alert (4-9 and 5-6). This is also taught in Cooper, such as in paragraph 594

As per claim 8, Cooper teaches wherein the interface includes a details control that allows a user to observe details about a selected anomaly (Figures 26 and 27, wherein a view button is available to view details).

As per claim 9, Cooper teaches wherein the details control presents a list of IP addresses to which the host attempted to connect (Figures 27, 29, 30 and throughout the reference).

Independent claim 22 is rejected using the same basis of arguments used to reject claim 1 above.

Claim 23 is rejected using the same basis of arguments used to reject claim 2 above.

Claim 24 is rejected using the same basis of arguments used to reject claim 7 above.

Claim 25 is rejected using the same basis of arguments used to reject claim 8 above.

3. Claims 10-14 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper and Symantec as applied above, and further in view of Billhartz US Patent No. 6,986,161 (hereinafter Billhartz).

Independent claim 10 is rejected using the same basis of arguments used to reject claim 1 above. However, Cooper and Symantec do not explicitly teach an event severity having a percentage relationship to an established threshold for issuing an event notification. This is taught throughout Billhartz though, such as in col. 8 line 41 to col. 9 line 10.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include basing event notifications on percent relationships. One of ordinary skill in the art would have been motivated to perform such an addition to provide greater certainty when issuing alerts, thereby reducing false positives. As indicated in col. 2

liens 15-23 of Billhartz, the previous intrusion detections systems do not reliably indicate whether some nodes are rouge or legitimate nodes.

As per claim 11, Symantec teaches an event to be snoozed for a fixed period of time (pages 4-9, 5-6, and 5-7).

Claim 12 is rejected using the same basis of arguments used to reject claim 2 above.

Claim 13 is rejected using the same basis of arguments used to reject claim 7 above.

Claim 14 is rejected using the same basis of arguments used to reject claim 8 above.

As per claim 18, as best understood by the Examiner, details of source and destination populated with IP addresses is taught throughout Cooper, as can be seen in Figures 23. Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.

4. Claims 15-17 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Porras US Patent No. 6,321,338 (hereinafter Porras).

As per claim 15, the Billhartz combination teaches all of the previous limitations, and the GUI interface for detecting intruders. However, it does not teach indicating normal operating conditions of a host and current operating conditions of a host.

Comparing these two are taught throughout Porras, such as in col. 2 lines 25-35; col. 6 lines 39-60; and col. 8 line 65 to col. 9 line 7.

At the time of the invention, it would have been obvious to combine the teachings of Porras with the Billhartz combination. Porras teaches creating long term statistical profiles ('normal' operating conditions), and comparing them with short term statistical profiles ('current' operating conditions). By doing so, network intrusion can be detected with greater accuracy and would provide greater security to networks (col. 2 lines 40-68).

As per claim 16, Porras teaches a comparison between normal and current connection rates of the host (col. 6 lines 1-20). The displaying of such features is taught by the Billhartz combination, as indicated earlier.

As per claim 17, Porras teaches throughout the reference events such as historical anomaly, as it compares previous long term statistical profiles. Porras also teaches event types like worm propagation, such as in col. 4 lines 25-48. Further, Porras teaches event types such as denials of service (col. 1 lines 55-65, col. 13 line 60-col. 14 line 7). Cooper teaches unauthorized access throughout the reference, and for example, can be seen in Figure 22.

As per claim 21, as best understood by the examiner, Porras teaches wherein a statistical measure is a number of bytes per second and packets per second of each type of protocol observed in the system (col. 5 lines 30-37).

5. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Central Point's *Central Point Anti-Virus – Virus detection, Removal and Prevention*, 1991 (hereinafter Central Point).

As per claim 19, the Billhartz combination does not explicitly teach displaying actions taken by the operator for the particular event. However, this is taught by Central Point, on pages 46-47.

At the time of the invention, it would have been obvious to combine the teachings of Central Point with the Billhartz combination. One of ordinary skill in the art would have been motivated to perform such an addition to create such records for data logging and for future references. This is taught on page 46 of Central Point, where it teaches that logs may be used for future references.

6. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Kuroshita US Patent No. 5,550,807 (hereinafter Kuroshita).

As per claim 20, displaying network statistics is taught throughout Cooper, such as in Figure 20. Although the Cooper combination teaches displaying many different statistics, the references do not explicitly teach displaying a ranking of hosts in the network according to a network statistical measure. Ranking hosts according to

network statistical measures are taught by Kuroshita though, such as in col. 1 line 34-52.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of Kuroshita with the Cooper combination. One of ordinary skill in the art would have been motivated to perform such an addition to manage the network and standardizing a network management protocol.

(10) Response to Argument

1) Claims 1-9 and 22-25 are not patentable over Cooper and Symantec

a) Cooper reference – Events and Summary of Anomalies

The Appellants first argue that Cooper does not teach the claimed feature of a "summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event." More specifically, the Appellants argue that the Cooper reference does not depict an event summary and does not summarize anomalies that generated the event. However, the Appellants have interpreted the claim language too narrowly, and the Cooper reference do teach such limitations.

Figure 26 of Cooper depicts a page alerting the user of events and associated anomalies. As can be seen on Figure 26, multiple events are alerted to the user. This alerting page is entitled "Events Summary." On the Table depicted in Figure 26, multiple events are listed. The events are listed under the column in the table entitled

"Type." For example, "ACCESS_VIOLATION" and "SECURITY ATTACK" are examples of events.

The Summary of Anomalies of each event is listed to the left of each event. For Example, for the first event, "ACCESS_VIOLATION," the summary is "Unauthorized_Acess_To_URL." Also, note that there are 5 counts (times that this has happened). Therefore, the "Disposition" and the "Count" columns are the summary of anomalies generating the event.

As clearly depicted in Figure 26 of Cooper, multiple events are listed, and each event is summary of anomalies are listed to the left of the event.

For even further evidence, the Appellant themselves admit that Cooper teaches events. As seen in the arguments for Claims 4 and 25, the Appellant themselves recite "Appellant maintains that Cooper teaches events, but did not teach anomalies used to classify the events."

b) Symantec Reference – Alert Region with Snooze Feature

The Appellants then argue that Symantic does not explicitly teach an "alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time." More specifically, the Appellants argue that the Symantec reference does not snooze alerts for a "period of time." However, the Office maintains that Symantec do teach such limitations.

As can be seen in Symantec on 4-8 and 4-9, a user can select a "Remember" function on the alert. Symantec on 4-9 recites "If the activity is valid ... and you don't want SAM to alert you of this activity in the future, click Remember... Clicking

Remember adds this activity to the Exceptions .... Future attempts ... will not trigger the suspicious activity alert .... see ... Chapter 5 for more information." In Chapter 5, Symantec further goes on to teach on 5-7 that "You can remove exceptions you no longer need or want."

As seen in the cited areas of Symantec, a user can snooze future alerts for a "period of time," and this time is based upon when the user removes the specified alert form an exception list.

c) Motivation to Combine

The Appellants continue to argue that there is no motivation to combine the Symantec and Cooper references. However, as stated in the previous Office Action, "One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity." The Appellants argue that there is no basis for the conclusion that it would be beneficial to snooze alerts because not all alerts are malicious. However, this is clearly stated in 5-6 of Symantec. This reasoning is not ex-post. As seen in 5-6 of Symantec, "If a suspicious activity is detected, it does not necessarily mean that a virus is performing the activity - you will decide whether the activity can continue or not ... For example ... you want the action to continue because it is valid in the context of the application you are running. "

d) Claims 2 and 23

The Appellants argue that the references do not teach that security policies are based on roles of hosts. However, this is clearly taught in Cooper, as cited in the Office Action. Cooper, in paragraph 100, teaches how policies may be generated in regards to security events and alerts. This paragraph recites "The wizard enables the end user to generate policy based on what can be considered gross characteristics of a network at the IP level, such as, for example ... communities of hosts." As seen in this passage, the policy information regarding security alerts and actions may be based on event and host based policies.

e) Claims 4 and 25

The Appellants continue to argue that the references do not teach the limitations of Claims 4 and 25. Claims 4 and 25 include limitations wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event. The Appellant points to the Examiner's Arguments, which points to Figure 12 of Cooper. The Appellant was correct in realizing that Figure 12 was a typographical error, but incorrect in interpreting the Figure to refer to Figure 21. The Examiner meant to refer to Figure 22. This should have been clear and evident, as the Office Action refers to Figure 22 in the 103 Rejection, and not to Figures 12 or 21. The Appellants ignore the rejection in the Office Action itself. As seen in Figure 22 of Cooper, the events are listed under the column "Type." The anomalies that classify the event are located to the left of the event, such as the information found in the "Count" and "Disposition" columns. For example, for the first event, "ACCESS_VIOLATION," the anomalies that classify the event are "5 counts of "unauthorized_access_To_Url."

As clearly depicted in Figure 22, which was recited to in the Office Action, Cooper does teach such claim limitations.

2) Claims 10-14 and 18 are not patentable over Cooper and Symantec

As per these claims, the Appellant argue that the claims should be allowable for the same reason as claim 1 above. However, the same arguments the Office as presented earlier applies to these claims as well.

Further, the Appellant argues that the references do not teach that an event severity is determined for the event, by the event having a percentage relationship to an established threshold for issuing an event notification.

As seen in Figure 26 of Cooper, there is a column entitled "Severity" which classifies the event severity. As seen, there are examples of CRITICAL, HIGH, and MEDIUM. Although the term "percentage" is not explicitly recited in Cooper, such warnings inherently involve percentages when there are multiple levels of warnings. As seen in the classification system utilized by Cooper, Cooper users multiple levels of severity. In such classification involving levels, a threshold must be met in order for an event to jump to a higher level. These threshold must involve some type of ratios, which are directly related to percentages.

Further, the Billhartz reference is used to further clarify the use of percentages. As seen in col. 8 line 41 to col. 9 line 10, Billhartz teaches a threshold/percent system to generate alerts. Col. 8 lines 56 to col. 8 line 62 shows an example. As seen in this example, if a certain percentage of packets transmitted during a period of time are involved in a certain number of collisions, then an intrusion alert is generated.

Therefore, the Cooper combination does teach the limitations of these claims.

Claim 12

The same arguments applied to claim 2 apply for claim 12 as well.

Claim 18

As per claim 18, the Appellants argue that the references do not teach displaying event details including destination and source fields populated with IP addresses and role classification of the host in the network. However, Cooper does teach such limitations, as can be seen in Figures 9 and 23 and paragraphs 100 and 158, as cited in the Office Action. Further the display of the policy host may be further seen in Figure 10c, under the Description column.

3) Claims 15-17 and 21 are not patentable over Cooper, Symantec, Billhartz, and Porras

These claims are not allowable at least for the reasons discussed in claim 10.

4) Claim 19 is not patentable over Cooper, Symantec, Billhartz, and Central Point

These claims are not allowable at least for the reasons discussed in claim 10.

5) Claim 20 is not patentable over Cooper, Symantec, Billhartz, and Kuroshita

These claims are not allowable at least for the reasons discussed in claim 10.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Jason K. Gee

Conferees:

Kambiz Zand (SPE of 2434) and Nasser Moazzami

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436